REMARKS

The above amendment and these remarks are responsive to the Office action of 26 Mar 2004 of Examiner Linh L.D. Son.

Claims 1-22 are in the case, none as yet allowed.

35 U.S.C. 101

Claims 8, 9, 10, 11, 12, 16, 17, and 21 have been rejected under 35 U.S.C. 101.

The Examiner asserts that the language of these claims "raises a question as to whether the claim is directed merely to an abstact idea that is not tied to a technological art, environment or machine."

Applicants traverse.

With respect to claims 8, 9, 10, 11, 12, and 21, the Examiner assets that the "claimed steps of configuring do not require a program or software to carry out the task. It is an abstract idea."

Specific hardware elements are recited in these claims, as is their management. It is not a requirement that a program or software be recited to carry out the steps of a method which is, as is the case here, operating on hardware elements.

In claim 8, 9, 10, 11, 12, and 21, the hardware elements recited include virtual private network (VPN) connections. The VPN connection, in particular, is clearly described in Applicants' invention as a hardware element. See Figure 2, and the description of VPN technology at page 2, lines 8-17 which clearly establishes the hardware nature, within the context of the Internet and computing industry, of the term VPN.

With respect to claim 16 and 17, the Examiner states that the claimed systems for operating and configuration are not tangibly embodied, that claim 16 does not include software operating on a medium or hardware, and that claim 17 does not disclose hardware.

Claim 16 recites a VPN connection, which is clearly hardware, as previously explained.

Claim 17 recites a database, VPN connections and address pools. A pool is a hardware element for storing addresses in an electronic database in an Internet environment, and this claim relates to configuring such a pool. See Applicants' Figure 2, element 48.

35 U.S.C. 102

Claims 14 and 15 have been rejected under 35 U.S.C. 102(e) over Borella et al. (U.S. Patent 6,353,614, hereinafter Borella).

Applicants have amended claims 14 and 15 to recite the virtual private network aspect of the claim, which claims relate thereby to the combining of IP Security (AH and ESP processing) with network address translation (NAT), and have clarified that the claimed matter executes at one end of the VPN connection.

Borella provides a method and protocol for Distributed NAT ("DNAT"), which is used to overcome the limited 32-bit address space of IPv4. The protocol includes a port allocation protocol and translates ports as well as IP addresses. Local ports are replaced with globally unique ports, unique for the scope of DNAT. Hence, Borella employs what is often referred to as 'PNAT' meaning 'port & network [IP] address translation'.

So, the two major differences between Borella and Applicants' invention are;

a) The subject invention does not translate port (transport layer 'address') at all. The reason this is undesirable is because some classes of important IP traffic does use TCP or UDP, hence the datagrams have no port numbers. These cannot be handled via a PNAT scheme. In contrast, VPN NAT handles all IP protocol traffic.

b) DNAT is a form if PNAT that centralizes the assignment and allocation of ports. Borella et all has nothing to do with IP Security or the IP Security protocols ESP & AH. This is critical since the incompatibilities and difficulties of combining of IP Security & NAT are well known (see, for example, IETF RFC3715). Hence Borella et al does even begin to address any of the problems associated with combining IP Security and NAT.

35 U.S.C. 103

Claims 1, 12, 13, 16, 18, 19 have been rejected under 35 U.S.C. 103(a) over Borella in view of Jain et al. (U.S. Patent 6,047,325, hereinafter Jain).

IP security is provided in a virtual private network using network address translation (NAT) by performing one or a combination of the four types of VPN NAT, including VPN NAT type 'a source-outbound' IP NAT, VPN NAT 'b destination-outbound', VPN NAT type 'c inbound-source' IP NAT, and VPN NAT type 'd inbound-destination' IP NAT. This involves dynamically generating NAT rules and associating them with the manual or dynamically generated (IKE) Security Associations, before beginning IP security that uses the Security Associations. Then, as IP Sec is performed on outbound and inbound datagrams, the NAT function is also performed.

The 4 types of VPN NAT are defined in Table 1 and with respect to Figures 5-7. The current invention concerns the ability to define and process multiple VPN NAT rules for a single VPN connection, via the specification of multiple IP addresses (an IP address set) for types of VPN NAT. The term 'VPN' here is used to refer to the IP Security protocols ESP (Encapsulating Security Payload) and AH (Authentication Header). Basic references for these protocols are (all from IETF (Internet Engineering Task Force)); IKE RFC2409 , ESP RFC2406, AH RFC2402, and the most basic, on architecture RFC2401. (See Applicants' specification, page 3, lines 11-17, and page 7, line 21 to page 8, line 1). The subject invention works over LANs and WANs, including wireless; it works where ever IP traffic works. And it is embodied in only one end of the VPN connection; the VPN implementation at the other end is completely unaware that its peer is performing VPN NAT operations.

Applicants' invention allows integration of VPN & NAT by logically performing the NAT operation *prior to beginning* the IKE negotiation of Security Associations. Hence the IKE negotiation begins and proceeds with the NAT IP address(es), rather than actual IP address(es). Any possible IP Sec protocol that is applied to a datagram to encrypt or sign a datagram works at both ends, because IP Sec and the Security associations are using the NAT address(es).

Borella provides a method and protocol for Distributed NAT ("DNAT"), used to overcome the limited 32-bit address space of IPv4. The protocol includes a port allocation protocol and translates ports as well as IP addresses. Local ports are replaced with globally unique ports, unique for the scope of DNAT. Hence, Borella employs what is often referred to as 'PNAT' meaning 'port & network [IP] address translation'.

So, the two major differences between Borella and Applicants' invention are;

a) The subject invention does not translate port (transport layer 'address') at all. The reason this is undesirable is because some classes of important IP traffic do use TCP or UDP, hence the datagrams have no port numbers. These cannot be handled via a PNAT scheme. In contrast Applicants' invention, VPN NAT, handles all IP protocol traffic.

b) DNAT is a form if PNAT that centralizes the assignment and allocation of ports. Borella has nothing to do with IP Security or the IP Security protocols ESP & AH. This is critical since the incompatibilities and difficulties of combining of IP Security & NAT are well known (see, for example, IETF RFC3715). Hence Borella does even begin to address any of the problems associated with combining IP Security and NAT.

Jain provides a network device which translates addresses and ports and filters packets at the link, network and transport layers. The invention uses a table (one of three mentioned) to bind MAC and IP addresses, via ARP (Address Resolution Protocol). The invention does say that traffic can be encrypted and authenticated when the traffic is sent over a wide-area-network

Differences between Jain and Applicants' invention are;

a) Applicants' invention does not translate port (transport layer 'address') at all. The reason this is undesirable is because some classes of important IP traffic do use TCP or UDP, hence the datagrams have no port numbers. These cannot be handled via a PNAT scheme. In contrast, VPN NAT handles all IP protocol traffic.

b) Applicants' invention does not use APR or MAC addresses at all, and solves the functional combination of IPsec-based VPN and NAT in a manner completely different than Jain. This is illustrated by the observation that both ends of Jain et al (Fig 1, 26 & 28) must embody Jain et al, while for the subject invention, only one end of the peer VPN connection embodies the subject invention.

Applicants' have amended all claims to clarify that IP Security and NAT is combined in such a way as to execute at one end only of a VPN connection, and thus distinguish Jan and Borella.

SUMMARY AND CONCLUSION

Applicants urge that the above amendments be entered and the case passed to issue with claims 1-22.

The Application is believed to be in condition for allowance and such action by the Examiner is urged. Should differences remain, however, which do not place one/more of the remaining claims in condition for allowance, the Examiner is requested to phone the undersigned at the number provided below for the purpose of providing constructive assistance and suggestions in accordance with M.P.E.P. Sections 707.02(j) and 707.03 in order that allowable claims can be presented, thereby placing the Application in condition for allowance without further proceedings being necessary.

Sincerely,

E. B. Boden, et al.

By

Shelley M Beckstrand

Shelley M Beckstrand
Reg. No. 24,886

Date: 24 June 2004

Shelley M Beckstrand, P.C.
Attorney at Law
61 Glenmont Road
Woodlawn, VA 24381-1341

Phone: (276) 238-1972
Fax: (276) 238-1545